



NOTICE OF RIGHT TO SUE WITHIN 90 DAYS

VIA EMAIL

150 M Street, N.E.
Karen Ferguson, EMP, 4CON, Room 9.514
Washington, DC 20530

August 16, 2022

Mr. Jonathan Jones
c/o Charles A. McKinney, Esquire
Law Offices of Charles A. McKinney
Talbott Tower
118 W. First St., Ste. 618
Dayton, OH 45402

EXHIBIT A

Re: EEOC Charge Against Ohio Dept. of Public Safety, Law Enforcement Administrative Data System

No. 532202000549

Dear Mr. Jones:

Because you filed the above charge with the Equal Employment Opportunity Commission, and more than 180 days have elapsed since the date the Commission assumed jurisdiction over the charge, and no suit based thereon has been filed by this Department, and because you through your attorney have specifically requested this Notice, you are hereby notified that you have the right to institute a civil action under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. 2000e, et seq., against the above-named respondent.

If you choose to commence a civil action, such suit must be filed in the appropriate Court within 90 days of your receipt of this Notice.

The investigative file pertaining to your case is located in the EEOC Cincinnati Area Office, Cincinnati, OH.

This Notice should not be taken to mean that the Department of Justice has made a judgment as to whether or not your case is meritorious.

Sincerely,

Kristen Clarke
Assistant Attorney General
Civil Rights Division

by /s/ Karen L. Ferguson
Karen L. Ferguson
Supervisory Civil Rights Analyst
Employment Litigation Section

cc: Cincinnati Area Office, EEOC

Ohio Dept. of Public Safety, Law Enforcement Administrative Data System



**Department of
Public Safety**

EXHIBIT B

Mike DeWine, Governor
Jon Husted, Lt. Governor

Thomas J. Stickrath, Director

Position Statement

Jonathan Jones v. ODPS- Law Enforcement Administrative Data System (LEADS)

Charge No. COL71 (48665)05232021 22A-2021-01911C

SUMMARY OF POSITION

On or about June 4, 2021, Jonathan Jones (hereinafter “Charging Party”) signed a complaint with the Ohio Civil Rights Commission against the Ohio Department of Public Safety, as the repository for and staffing agency of Ohio’s Law Enforcement Automated Data System (LEADS) (“Respondent”) alleging he has been discriminated against due to race, color and gender. Respondent has not violated Ohio Revised Code 4112.02 (it was not Charging Party’s employer or prospective employer), nor Respondent’s policies regarding discrimination and retaliation (Exhibit A). Charging Party already submitted Charge No. 532-2020-00549 on January 16, 2020 to both the Commission and the Equal Employment Opportunity Commission (EEOC), which covers the same alleged wrongdoing and is currently under investigation by the EEOC. Respondent provides this response to the current charge, which appears to be Charging Party’s attempt to provide additional information relating to the EEOC investigation, but reserves all arguments and rights relating to the 2020 charge, including, for example, those relating to a competing, preexisting investigation by the EEOC, the limitations on time within which to file a charge, and limitations on amending a prior charge.

RESPONDENT’S REPLY TO CHARGING PARTY’S ALLEGATIONS

Though the Commission lacks jurisdiction under Ohio Revised Code Chapter 4112 over Respondent for this Charge, Respondent’s actions were reasonable, based on the specific facts at hand, and nondiscriminatory. Before turning to Charging Party’s allegations, however, the Commission may benefit from a fuller understanding of LEADS. Ohio Revised Code § 5503.10 establishes the distribution system for confidential, law enforcement information at issue in this Charge:

5503.10 Law enforcement automated data system.

There is hereby created in the department of public safety, division of state highway patrol, a program for administering and operating a law enforcement automated data system, to be known as LEADS, providing computerized data and communications to the various criminal justice agencies of the state. The program shall be administered by the superintendent of the state highway patrol, who may employ such persons as are necessary to carry out the purposes of this section. The superintendent shall adopt rules under Chapter 119. of the Revised Code establishing fees and guidelines for the operation of and participation in the LEADS program. These rules shall include criteria for granting and restricting access to information maintained in LEADS.

Among rules adopted for the implementation of LEADS is Chapter 4501:2-10 of the Ohio Administrative Code. Section 4501:2-10-06(C) says: "Messages and/or throughput of any kind accessed through LEADS shall be restricted to the use of duly authorized law enforcement and/or criminal justice agencies for the administration of criminal justice." Access to and dissemination of LEADS throughput is governed by the LEADS security policy (8/3/2020) and LEADS manual (2021) available at <http://leads.ohio.gov/Manuals>." LEADS is the access point for multistate criminal justice information:

LEADS was not designed only to provide criminal justice information to law enforcement agencies *within* the State of Ohio. LEADS was also intended to form a vital component of the National Crime Information Center (NCIC) operated by the Federal Bureau of Investigation (FBI) in Clarksburg, West Virginia. NCIC maintains computer files of information provided by each of the fifty states. LEADS users in Ohio can access NCIC files through LEADS, just as users in other states can access NCIC files through their own states' systems. Thus, LEADS provides criminal justice information from across the country to Ohio law enforcement agencies and, at the same time, provides criminal justice information from Ohio to law enforcement agencies across the country.

LEADS Manual, at p. 3. Because LEADS includes access to both state and federal information, then, both state and federal security policies and operation manuals govern access to information. *See e.g.*, 28 C.F.R. §§ 20.1 *et seq.*; U. S. Department of Justice, Federal Bureau of Investigation "Criminal Justice Information Services (CJIS) Security Policy" (6/20/2020).

One source of restriction to both the state and federal confidential law enforcement information is the LEADS Security Policy on Personnel Security, which provides in part:

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the LEADS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

- a. 5 CFR 731.106; and/or
- b. Office of Personnel Management policy, regulations, and guidance; and/or
- c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix K for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. ***If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.***
 - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. ***Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.***
 - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.
4. ***If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.***
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. ***If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.***
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.
8. ***The agency may appeal the decision of the CSO, or his/her designee, by submitting a letter from the agency administrator outlining the following items:***
 - a. The applicant's name, date of birth and OLN.
 - b. An explanation as to why an appeal should be granted.
 - c. The statement "This agency has internal policies governing the use of LEADS and CJIS system access and the employee will be held accountable to these policies and all LEADS administrative rules. I, as the agency administrator, accept ultimate responsibility for this employee's actions in the use of LEADS".

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

LEADS Security Policy, § 5.12 at pp. 67-68 (emphasis added). Further, Ohio Administrative Code § 4501:2-10-01(OO) specifies that:

"Serious misdemeanors," for the purpose of being a terminal operator, include but are not limited to the following:

- (1) Any offense classified by the Ohio Revised Code as a misdemeanor of the first degree;
- (2) Any offense which involves a crime against a person in which physical harm or the threat of physical harm occurred;
- (3) Any offense involving the use/misuse of a computer or computer system;
- (4) Any offense involving theft, identity theft, fraud, or other similar offense;
- (5) Any offense involving the impersonation of a law enforcement officer;
- (6) Any offense where the use of LEADS information was instrumental in the commission of the offense.

Taken together, and as explained below, when the LEADS administration staff identifies a prospective or current user with a serious misdemeanor, such as domestic violence with accompanying threats of or actual harm to the victim, or when – in addition – the applicant did not appear forthcoming about the nature or extent of the situation or another similar incident, then, regardless of whether the applicant pled to a lesser offense thereby avoiding a conviction for domestic violence or a sex offender designation, LEADS can reasonably deny access to LEADS information.

- I. **Was denied an opportunity for computer access that is required to do the functions of a police officer for an arrest with no conviction that happened in 2005 and expunged under ORC 2953.52 in 2007. BCI states that BCI record should not have been used as there was no disposition and no judicial portion contained within the BCI report. LEADS also used an earlier arrest to deny access to system based on a previous arrest in 2003 in which I was the victim of the assault, where my case was dismissed but the other person was found guilty and to date is not eligible for expungement. BCI report was not updated and for the reasons of denial which cost me my job, for arrest. In my possession are documents from LEADS of a white male who was arrested for the same charge 12 prior to having his access suspended. In this letter LEADS wanted to know his disposition, and not mine. Both have same expungement and not found guilty. He did not violate their rules but I did. Same issue with a White CPD arrested for DV. She was not found guilty of just as I but she retained her access to the database and did not violate any rules, only I did. Sgt. James Scott and Officer Rose Valentino of the CPD.**

In the first place, this Charge is misplaced because Respondent was not Charging Party's employer/potential employer under Revised Code Chapter 4112, therefore we are unable to provide a copy of the application for employment used for employment. The Charge itself makes clear that Charging Party sought a position with the Cincinnati Police Department (CPD). The Ohio Department of Public Safety is an instrumentality of the State of Ohio. The Ohio State Highway Patrol is a division of the Department, and also an instrumentality of the State. LEADS, under the Highway Patrol, simply is not part of the City of Cincinnati or otherwise involved in the employment decisions of any of the many municipalities, political subdivisions, and law enforcement agencies that seek access to LEADS information, and therefore cannot provide policies relating to the screening, hiring, firing, qualifications and disqualifications of applicants for CPD, as well as a record of applicants who applied for the same position with CPD as Charging Party within the last two years. Neither the Ohio State Highway Patrol that houses LEADS, nor the United States Department of Justice that controls NCIC, were part of the "management" of the CPD. LEADS does not make any recommendation to CPD on whether they should or should not hire a prospective employee. As set out in more detail below, CPD

inquired whether Respondent would allow its prospective employees – Charging Party and the others – access to confidential, law enforcement information through LEADS. LEADS applied its access criteria, and responded accordingly. LEADS was never Charging Party’s prospective employer. As a result, the Commission should reject Charging Party’s invitation to improperly exercise its jurisdiction over this Respondent on the facts of this Charge. Furthermore, Charging Party’s suggestion that direct access to LEADS is “required to do the functions of a police officer” is not accurate. LEADS is a resource for law enforcement agencies. Not all law enforcement agencies in Ohio are LEADS agencies. Not all officers have LEADS access. Some may use, instead, the Ohio Law Enforcement Gateway (OHLEG) offered by the Ohio Attorney General’s Office. Some agencies may not require access to either system. Some positions, perhaps even within agencies that are LEADS agencies, may not require access.

Even though the lack of an employment relationship is enough to result in a finding of no probable cause of discrimination, regardless, Charging Party was not singled out by, or treated differently because of, his race, color or gender. On November 8, 2019, CPD’s LEADS Terminal Agency Coordinator (TAC) Sheila Bond sent an email to LEADS with a list of potential CPD employees. TAC Bond forwarded candidates’ names and records, and requested a review of each candidate’s criminal record and a decision on granting LEADS access. LEADS Program Administrator Kara Joseph also ran a criminal history on each candidate. She requested additional information from TAC Bond relating to the records for Charging Party.

On November 13, 2019, TAC Bond sent Ms. Joseph some of the requested documents – a portion of a 2005 police report, a portion of the Charging Party’s application with CPD describing that 2005 incident, and a portion of Charging Party’s polygraph examination. The polygraph asked Charging Party to “explain in detail any physical confrontations in which you were involved with a spouse, parent, or other family member, boyfriend, girlfriend, or other family member [sic].” Charging Party described a 2005 incident, corresponding to the 2005 portion of a police report, which documented an injury to the victim/other participant in the altercation, his girlfriend at the time. The report went further, though, reciting her claim that Charging Party “jumped on her back and took her to the ground with a headlock,” and “further stated that [Charging Party] began to choke her when he got her to the ground” then stating she “had a small amount of blood on her shirt. It appears to come from her bottom lip.” Neither Charging Party’s response in the polygraph nor the records from CPD addressed an earlier arrest that Ms. Joseph uncovered and inquired about. LEADS Administrator John Moore reviewed all documentation and denied access according to LEADS standards based on the police report, polygraph report, arrest in 2005, and earlier incident that Charging Party had not disclosed but which the LEADS team uncovered. LEADS emailed TAC Bond copies of the letters (denial and approval of LEADS access) for each candidate. In Charging Party’s denial, LEADS stated the agency could appeal the decision. (Exhibit B.)

Charging Party’s access to confidential state and federal law enforcement information had nothing to do with his race, color or gender. Charging Party states the Bureau of Criminal Investigation (BCI) record should have been updated. First, BCI is an arm of the Ohio Attorney General’s Office. Respondent cannot speak to what BCI “should” have done or what information it had available to it. Second, Respondent has not received an order sealing Charging Party’s criminal record pursuant to Ohio Revised Code 2953.52-53. (While Charging Party claims that his criminal record relating to at least one of his past criminal incidents has been “expunged,” the statute he cites relates to sealing the record and retaining an index of the record so that, in the proper circumstance, the record can still be reviewed.) Third, Respondent received and reviewed information directly from CPD’s TAC, not just a criminal history. And, Respondent did, in fact, receive and review records relating to Charging Party’s criminal history. The charge challenges Respondent’s actions in 2019, when the information was, in fact, available to it. If circumstances have changed, or if, as it appears, Charging Party is primarily concerned about what may happen should he apply for a law enforcement position again, and his prospective

employer makes a LEADS access inquiry when those records are no longer on his criminal history, then that concern exceeds the scope of the charge.

Respondent simply did not make its 2019 determination regarding Charging Party because of his race, color or gender. Respondent cannot speculate as to the records in Charging Party's possession, or his personal beliefs, for example on how the claims were resolved, sealed, or eligible to be sealed. Looking to the two people he does identify, though, he is not similarly situated to them. One day after LEADS Administrator Moore sent CPD notice of Charging Party's denial of access, Mr. Moore sent another letter to CPD revoking access for a Caucasian Sergeant already at CPD who was arrested on the same charge as Charging Party, Sgt. James Scott (Exhibit C.) Even though this shows that at the very same time as Charging Party's denial, LEADS was administering access uniformly regardless of race, what is more is that it does not appear that LEADS Administrator Moore was even aware of Charging Party's race or color when Moore made the decision not to extend access. Furthermore, Charging Party was not a current user, but Scott and Valentino were. And, perhaps most importantly, the decision as to Charging Party was not based solely on a criminal history. His decision included, among other things, a second arrest which he failed to disclose – which made both the arrests and lack of candor relevant to the determination. As for Rose Valentino, she too was a current officer and not similarly situated to Charging Party. As one would expect, Respondent reviewed the officer's case on the specific facts, including the plea to a misdemeanor. On her circumstances, she was granted access to LEADS. It bears repeating that neither Sgt. James Scott nor Officer Rose Valentino were employees or potential employees of the Department of Public Safety, and therefore Respondent is unable to provide copies of their employment applications or demographic information.

Cincinnati Police Department had the right to appeal all denials to access LEADS. LEADS has no appeals on file from the Cincinnati Police Department relating to Charging Party. When Sgt. Scott was later acquitted of the charges against him, his employer asked that his access be reinstated, and LEADS accommodated that request. Had circumstances been different – for example, had CPD appealed the determination relating to Charging Party, had Charging Party revealed all the arrests in his background, or had different records been provided to Respondent – then perhaps the result would be different. That result, however, was not because of Charging Party's race, color, or gender.

Respondent was not Charging Party's actual or prospective employer, and did not discriminate against Charging Party based on his race, color or gender. Charging Party omitted pertinent information from his employment application and background check. The Department's denial of LEADS access was based on a particularized review of his criminal record and consistent with other denials, including one for a Caucasian officer whose access to LEADS shut off the day after it denied Charging Party's access for the same offense of domestic violence. Charging Party, or perhaps even the Commission, may not agree with LEADS, the Highway Patrol, Ohio Department of Public Safety, FBI, or Department of Justice about the strictness of the standards used to decide who will have access to vital and confidential criminal justice information. Such disagreement, though, does not show discrimination; and, that is especially so where, as here, decisions are based on a reasonable and particularized review of each applicant that is applied regardless of race, color or gender.

Respondent does not discriminate in any way contradictory with the laws of the United States or the State of Ohio on the basis of race, sex, color, religion, age, national origin, sexual orientation, gender identity or disability.

Should additional information or allegations arise during the course of Commission's investigation, Respondent requests the opportunity to respond.

Based on the foregoing, Respondent respectfully requests a no probable cause finding with respect to Charging Party's charge of discrimination.

Respectfully Submitted,

Toby Chambliss EEO Officer
1970 W. Broad St
Columbus Ohio 43223
tdchambliss@dps.ohio.gov

Date: August 11, 2021